

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY**

UNITED STATES OF AMERICA,

v.

**FELIX ROQUE and
JOSEPH ROQUE,
a/k/a “Maria Pasquale”
a/k/a “Jeffery Reynoso”**

Criminal No. 12-540 (KM)

MEMORANDUM OPINION

Before the court are omnibus pretrial motions by defendant Joseph Roque, joined (I assume) by Felix Roque. When filed, the motions were directed to the face of the Indictment, but they were supplemented to address the subsequently-filed Superseding Indictment [ECF 34]. I heard oral argument on June 3, 2013, and reserved decision. Because I write this short unpublished opinion primarily for the benefit of the parties, familiarity with the underlying facts and allegations is assumed.

Essentially, the Superseding Indictment¹ alleges that Felix Roque, who is the Mayor of West New York, and his son, Joseph Roque, sought, through violations of the Computer Fraud and Abuse Act (“CFAA”), to disable a website critical of Mayor Roque’s administration and to harass persons associated with the website. Of course, alleging is not proving, and the defendants are clothed in the presumption of innocence. It would be premature and inappropriate at this stage to consider the truth, or not, of what is alleged. The current motions are directed to the sufficiency of the Indictment and its allegations as a matter of law.

The Indictment currently contains two counts, summarized by the government as follows:

Count 1-the “Conspiracy Charge”

Conspiracy to:

¹ The Superseding Indictment, filed April 18, 2013 [ECF 34], is the currently operative charging document. For simplicity, it will be referred to in this Opinion as the “Indictment.”

- (1) gain unauthorized access to Hotmail, in furtherance of:
 - (a) damaging protected computers, contrary to 18 U.S.C §1030(a)(5)(A); and
 - (b) harassment, contrary to N.J.S.A. 2C:33-4(a) and (c) (the “New Jersey Harassment Statute”); and
- (2) gain unauthorized access to Facebook, in furtherance of harassment, contrary to the New Jersey Harassment Statute

All contrary to 18 U.S.C. §§ 1030(a)(2)(C) and (c)(2)(B)(ii), and in violation of 18 U.S.C. § 371.²

Count 2-the “Access Charge”

Unauthorized access to Hotmail, in furtherance of:

- (a) damaging protected computers, contrary to 18 U.S.C §1030(a)(5)(A); and
- (b) harassment, contrary to the New Jersey Harassment Statute

All in violation of 18 U.S.C. §§ 1030(a)(2)(C) and (c)(2)(B)(ii).

1. Challenge to Application of the CFAA on Tenth Amendment Grounds

Defendants move to dismiss the Indictment. They assert that the CFAA, at least as applied here, impinges upon the authority of the State of New Jersey to regulate local conduct, and hence violates the Tenth Amendment to the United States Constitution. The Tenth Amendment provides that “powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.” U.S. Const. amend. X. The government responds, in essence, that the CFAA is an exercise of a power “delegated to the United States by the Constitution” – specifically, by the Commerce Clause, which grants Congress the power to “regulate Commerce ... among the several States.” U.S. CONST. art. I, § 8, cl. 3. *See generally Treasurer of N.J. v. U.S. Dep’t of Treasury*, 684 F.3d 382, 413 (3d Cir. 2012) (“If Congress acts under one of its enumerated powers ... there can be no violation of the Tenth Amendment”)(quoting *United States v. Parker*, 108 F.3d 28, 31 (3d Cir. 1997)).³

² The conspiracy charge of the Indictment rests on the general conspiracy provision, 18 U.S.C. § 371, not on the CFAA conspiracy provision, 18 U.S.C. § 1030(b).

³ So formulated, the issue is simply the limit of the federal Commerce Clause power. Defendants suggest, however, that the Tenth Amendment has independent force and may limit the scope of even enumerated Constitutional

The CFAA was enacted pursuant to the Commerce Clause power. The CFAA charges here are explicitly tied to “protected computers,” defined as computers “used in or affecting interstate or foreign commerce or communication.” 18 U.S.C. § 1030(e)(2)(B). The Indictment alleges that each computer in question was a protected computer, *i.e.*, a “computer used in and affecting interstate commerce.” *E.g.*, Indictment Count 1, ¶¶ 2(a) & (b); Count 2, ¶ 2. If facially adequate, such allegations are sufficient to call for a trial on the merits. *See generally Costello v. United States*, 350 U.S. 359, 363 (1956); *United States v. Vitillo*, 490 F.3d 314, 320 (3d Cir. 2007). The Indictment, in other words, need only allege a valid offense; it need not on its face negate the possibility of every application of the statute that might present a Constitutional problem. It is almost tautological that an allegation of interstate commerce, if proven, would establish the required nexus to interstate commerce. And having alleged interstate commerce, the government has taken on the burden of proving it. Nevertheless, because that is something of a legal conclusion, I will entertain briefly the defendants’ contention that the allegations *factually* fall short of what is legally required to support federal jurisdiction. *See generally* FED. R. CRIM. P. 12(b)(3)(B); *United States v. Panarella*, 277 F.3d 678, 685 (3d Cir. 2002) (Rule 12 challenge available “if the specific facts alleged in the charging document fall beyond the scope of the relevant criminal statute”).

It is settled that the Commerce Clause power encompasses (1) the use of the channels of interstate commerce; (2) the instrumentalities of interstate commerce, or persons or things in interstate commerce; and (3) activities that substantially affect interstate commerce. *See United States v. Lopez*, 514 U.S. 549, 558-59 (1995); *United States v. Bishop*, 66 F.3d 569, 590 (3d Cir. 1995). The Indictment alleges facts and circumstances sufficiently broad to encompass proof of the requisite connection to interstate commerce under category (1) or category (2).

The inherent attributes of the internet, plus the physical locations of the computers in question here, suggest that the defendants used the “channels” or “instrumentalities” of interstate commerce, and that the relevant communications crossed state lines and hence were “in” interstate commerce. *See United States v. MacEwan*, 445 F.3d 237, 245 (3d Cir. 2006) (concluding

powers. Defendants point to the United States Supreme Court’s recent grant of *certiorari* in *United States v. Bond*, 681 F.3d 149 (3d Cir. 2012), *cert. granted*, 2013 U.S. LEXIS 914 (Jan. 18, 2013) (No. 12-158). One of the questions presented by *Bond* involves federalism-based limitations on a federal statute based on the Treaty Power, U.S. Const. art. II, § 2. I cannot, however, speculate as to why the Supreme Court granted *certiorari*, anticipate its decision, or presume to apply or distinguish its hypothetical reasoning.

that the “Internet is an instrumentality and channel of interstate commerce”); *United States v. Trotter*, 478 F.3d 918, 921 (8th Cir. 2007). The computers at issue here were all connected to the internet, and were used to communicate over the internet. The government argues, with some force, that the internet is the quintessential “instrumentality” of 21st century commerce. Thus the commerce power that once permitted the government to regulate intrastate activities of railroad cars would permit regulation here, even if the computer communications had been confined to this State. *Cf. Southern R. Co. v. United States*, 222 U.S. 20 (1911).⁴ Even as applied to in-state activity, the CFAA has been upheld as a valid exercise of the Commerce Clause power. *See, e.g., Trotter*, 478 F.3d at 921; *United States v. Mitra*, 405 F.3d 492, 496 (7th Cir. 2005) (purely local attack on first-responder network upheld as violation of CFAA because the network operated over the electromagnetic spectrum and was an instrumentality of interstate commerce). Likewise, and in the alternative, the commerce power that once permitted the government to regulate persons and property actually transported across state lines permits regulation of the interstate communications here. *Cf. Brooks v. United States*, 267 U.S. 432 (1925) (upholding Dyer Act, which prohibits transportation of stolen vehicles across state lines); *Hoke v. United States*, 227 U.S. 308, 320 (1913) (Mann Act). Actual interstate communications between, for example, computers in New Jersey and “Go Daddy, an Internet Service Provider (‘ISP’) located in Arizona,” or “Weebly, a second ISP located in California” (Indictment Count 1, ¶ 1(h)), may demonstrate that the computers were used “in” interstate commerce. *See Trotter*, 478 F.3d at 921 (citing *Mitra*, 405 F.3d at 496).

We might hypothesize that the offense conduct involves purely local politics, or that the participants were personally indifferent to the interstate character of the internet or the location of the servers. In general – and certainly at this pretrial stage – I cannot say that this affects the issue. It may be just as true, for example, that a carjacker does not intend to commercially exploit a stolen car, or to drive it across state lines; nevertheless, because carjacking implicates interstate commerce, Congress has the power to prohibit it. *See Bishop*, 66 F.3d at 590; *see also Trotter*, 478 F.3d at 922,

⁴ Thus it is unnecessary to address the most controversial and potentially far-reaching aspect of Commerce Clause jurisdiction: intrastate activities that “substantially affect” interstate commerce. *See, e.g., National Federation of Independent Business v. Sebelius*, 567 U.S. ___, 132 S. Ct. 603 (2012); *Gonzales v. Raich*, 545 U.S. 1 (2005); *Wickard v. Filburn*, 317 U.S. 111 (1942).

Defendants cite other authorities, such as “anti-commandeering” cases that limit the federal government’s ability to usurp the resources of state government for its own purposes. *E.g., New York v. United States*, 505 U.S. 144 (1992). These cases state generally applicable federalism concerns, but are not sufficiently on point to require dismissal of this Indictment.

Under these principles, I cannot grant defendants' motion to dismiss the Indictment. The allegations of the Indictment encompass a set of facts that, if proven, would make out a violation of the CFAA that would fall within the Commerce Clause power. Even if I accepted the defendants' Tenth Amendment reasoning, *see* n.3, above, I could not find at this early procedural stage that the government had boxed itself out of proving a valid federal case. The motion to dismiss the Indictment on these grounds is denied.

2. *Sufficiency of the Indictment under Rule 7(c)*

Defendants move to dismiss the Indictment for failure to state an offense.⁵ Rule 7(c), Fed. R. Crim. P., requires that an indictment contain a "plain, concise and definite written statement of the essential facts constituting the offense charged." The allegations of the Indictment must be accepted at face value for purposes of this motion to dismiss. The court will ask only whether the Indictment states the essential elements of the offense; sufficiently appraises the defendant of the allegations he must meet; and is sufficiently specific to permit the defendant to plead a former acquittal or conviction in the event of a subsequent prosecution. *See, e.g., United States v. Kemp*, 500 F.3d 257, 280 (3d Cir. 2007). This Indictment meets those standards.

Defendants argue that the Indictment fails to allege that they "obtained information" as a result of the acts charged in the Indictment. *See* 18 U.S.C. § 1030(a)(2)(C) ("Whoever ... intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information from any protected computer" shall be punished as provided in 18 U.S.C. § 1030(c)).

As to the Count 1 conspiracy charge, it is immaterial whether defendants allegedly succeeded in obtaining information. A valid conspiracy conviction does not require the accomplishment of the conspiracy's illegal object; it is very well settled that a section 371 conspiracy requires only an agreement to commit a substantive federal offense and an overt act in furtherance of that agreement. *E.g., United States v. Falcone*, 311 U.S. 205, 207 (1940); *Goldman v. United States*, 245 U.S. 474, 477 (1918); *United States v. Shoup*, 608 F.2d 950, 956 (3d Cir. 1979). The Indictment adequately alleges, for example, that "obtain[ing] information" from the West New York News Account and Facebook Account was part of the object of the conspiracy. (Indictment Count 1, ¶¶2(a), 2(b)). That is sufficient.

⁵ Certain of the grounds asserted in the original motion apply only to the original Indictment, and have become moot in light of the Superseding Indictment. That is by no means the defendants' fault; the Indictment was superseded after the deadline for filing of motions. I permitted the defendants to supplement their papers in light of the Superseding Indictment.

As to the substantive offense alleged in Count 2, the Indictment clearly alleges that the defendants, in a specified eleven-day period, “did knowingly and intentionally access a computer without authorization and exceed authorized access and thereby obtain information, that is, the contents of the West New York News Account, from a protected computer” (Indictment Count 2, ¶2) No more is required. Defendants argue that many or most of the acts of unauthorized access did not result in their obtaining information. Whether or not the proofs bear out that assertion, the Indictment does state an offense, and it will not be dismissed on that basis.

3. Challenges relating to “Damage”

Defendants seek to dismiss the Indictment because it fails to allege a viable claim of “damage” to protected computers, or because the “damage” provision is unconstitutionally vague. *See* 18 U.S.C. § 1030(a)(5)(A) (“[w]hoever ... knowingly causes the transmission of a program, information, code or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer” shall be punished as provided in 18 U.S.C. § 1030(c)). There is no substantive “damage” charge in the Superseding Indictment, a circumstance that requires some explanation.

Count 2 charges unauthorized access to a computer. An unauthorized access offense carries felony penalties of 5 years’ imprisonment and a fine if it was committed “in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.” 18 U.S.C. § 1030(c)(2)(B)(ii). Count 2 alleges that one such “criminal or tortious act” is a violation of the “damage” provision, 18 U.S.C. § 1030(a)(5)(A), quoted above. Count 2 also alleges a second, alternative “criminal or tortious act”: a violation of the New Jersey Harassment Statute.

Count 1 charges a conspiracy to commit the entire offense alleged in Count 2, including the Count 2 allegation that the unauthorized access to Hotmail was undertaken “in furtherance of” violations of the “damage” provision and the New Jersey Harassment Statute. Count 1 also charges that the conspiracy had an additional and alternative object: to gain unauthorized access to Facebook, in furtherance of a violation of the New Jersey Harassment Statute.

As to the conspiracy count, the government urges that under general principles of conspiracy law (noted in the preceding section), the defendant need not succeed in accomplishing the conspiracy’s object. That principle, says the government, applies to the intended “damage” here. *See* Gov’t Br. at 22, *citing United States v. Moran-Toala*, No. 09-cr-103 (FB), 2012 WL 748612, at *3 (E.D.N.Y. Mar. 8, 2012); *United States v. Kernell*, No. 3:08-cr-142, 2010 WL 1408438, at *6 (E.D. Tenn. Apr. 2, 2010). At oral argument it also became

clearer that, as to both the conspiracy count and the substantive count, the government maintains that “in furtherance of” means something akin to “in furtherance of *the goal* of.” That is, the federal or state violation need not be completed; the unauthorized access need only be done in furtherance of the accomplishment of, for example, “damage” to a protected computer.

At any rate, says the government, the Indictment does allege actual “damage” to a protected computer within the meaning of the “damage” provision. That provision defines “damage” very broadly as “*any* impairment to the *integrity* or *availability* of data, a program, a system, or information.” 18 U.S.C. § 1030(a)(5)(A) (emphasis added). See Gov’t Br. at 23-24, *citing I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc.*, 307 F. Supp. 2d 521, 525 (S.D.N.Y. 2004) (hacking password protected website); *United States v. Oddo*, 133 F. App’x 632, 633 (11th Cir. 2005) (redirecting website visitors to another website); *Int’l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 419-20 (7th Cir. 2006) (deletion of information from computer).

The defendants argue that merely “drawing a curtain” across data, rendering it inaccessible without actually destroying anything, should not be regarded as “damage.” But in light of the broad definition of § 1030(a), I cannot find that the allegations of the Indictment could not support proof of a valid charge. The Indictment alleges that Joseph Roque hacked into a password-protected account associated with the Recall website; that he cancelled the Go Daddy account, thereby removing users’ ability to access the site; and that he deleted website content. The allegations of the Indictment fit within the broad legal definition.

For the same reason, I reject any vagueness challenge at the present time. First of all, it is far preferable to consider such a challenge in the context of a factual record. I will not hypothesize marginal circumstances under which the statute’s applicability might be unclear; the proofs might establish that defendants’ acts lie in its heartland. See *generally United States v. Mazurie*, 419 U.S. 544, 550 (1975). More fundamentally, vagueness and breadth are not the same thing. The statutory definition of “damage” may be very inclusive, but it is not unclear. On a fair reading, it is apparent that it would apply to the activities alleged.

Finally, the Indictment alleges alternative bases for criminal liability: both counts allege acts in furtherance of state-law harassment. Those alternative bases would not be affected by the defendants’ “damage” arguments. For this reason, too, it is not critical to parse all of defendants’ arguments at the present time. It is clear that the Indictment pleads valid offenses, and should not be dismissed.

4. Challenge to the Enhancement Provision

Defendants challenge the application of the Enhancement Provision, 18 U.S.C. § 1030(c)(2)(B)(ii), which would elevate the unauthorized access offense from a misdemeanor to a felony punishable by 5 years' imprisonment. As noted above, that enhancement is based on the commission of the offense "in furtherance of any criminal or tortious act in violation of the Constitution or the laws of the United States or of any State." *Id.*

One of the charged "furtherance" objects, as noted above, is a violation of the "damage" provision, 18 U.S.C. § 1030(a)(5)(A). According to defendants, this is a form of bootstrapping. Offenses that may enhance the CFAA penalty, they say, should not include other offenses under the CFAA. The statute, however, specifically incorporates "any" offense or tort, state or federal; a more inclusive expression of intent can hardly be imagined.⁶

Also unpersuasive is defendants' argument that there is a "merger" problem with using a CFAA offense to enhance penalties, or that the incorporation of offenses renders the Enhancement Provision vague. The offense and the enhancement based on "damage" are not based on identical or self-proving conduct. The computer to which defendants gained access was the computer containing the West New York Account. The protected computers that they are accused of "damaging" are the Weebly and Go Daddy ISP servers. *See generally United States v. Cioni*, 649 F.3d 276, 283 (4th Cir. 2011) (no merger problem if access to separate computers were proven). At any rate, both the merger and vagueness claims must be approached with great caution in advance of the government's presentation of evidence.

I see no clear basis to exclude the "damage" offense from consideration or to dismiss the Indictment on that basis. There is no need to anticipate issues that the development of a factual record may alter or moot. I further note that state-law harassment is an alternative basis for enhancement of sentence, a basis that is unaffected by defendants' arguments here. I see no sufficient basis for dismissal at this time.

⁶ Defendants state that Congress knew how to incorporate other violations of CFAA when it wanted to, citing 18 U.S.C. § 1030(c)(4)(A), which specifically refers to "another offense under this section." But the (c)(4)(A) reference (like that in (3)(B)), refers *only* to violations of CFAA; it has to do with an accused's status, or not, as a CFAA recidivist. As such, it is not a fruitful comparison to the very inclusive Enhancement Provision at issue here.

5. Challenge to Indictment as Duplicitous

Defendants claim that Count 2, the access charge, is duplicitous, *i.e.*, that it impermissibly charges two or more crimes in a single count. *See United States v. Haddy*, 134 F.3d 542, 548 (3d Cir. 1998). The government has considerable latitude in choosing the appropriate unit of prosecution. And, as the government points out, the alternative may be to charge each incident of unauthorized access as a separate offense, magnifying defendants' culpability in the jury's eyes.

Count 2 concededly encompasses, or could encompass, multiple occasions on which defendants gained access to the West New York News account. All of those occasions, however, took place in a limited time span: February 6 through February 17, 2012. They seem to be interrelated. I do not think the allowable unit of prosecution has been exceeded here. The government has recognized that the inclusion of multiple incidents may require special care to ensure jury unanimity, and I agree; a "smorgasbord" verdict is not permissible.

6. Bill of Particulars

Closely related to the discussion in section 5, above, is defendants' request for a bill of particulars. Rule 7(f), Fed. R. Crim. P., grants the authority to require a bill of particulars. A bill of particulars will be granted where "an indictment's failure to provide factual or legal information significantly impairs the defendant's ability to prepare his defense or is likely to lead to prejudicial surprise at trial." *United States v. Rosa*, 891 F.2d 1063, 1066 (3d Cir. 1989). To my mind, the class of cases in which a bill of particulars should, or may, be granted is broader than the class of cases in which it must be granted. In one limited respect, related to Count 2, I will exercise my discretion to require a bill of particulars.

CFAA is very broad in scope, because it is designed to reach a wide range of criminal acts. The government has appropriately invoked the breadth of the statute to preserve the Indictment from dismissal. *See* sections 1-5, above. But that enforcement flexibility may carry with it a duty of extra care to define the scope of the charges in a particular case.

We are now on the brink of trial, which is scheduled for July 23, 2013. The theory of the case should be, and I have no doubt is, settled. To be sure, the conspiracy count is detailed, and I also take the prosecutors at their word that they have provided ample discovery. Moreover, because conspiracy is an inchoate offense, I do not think it would be appropriate to require the government to articulate a theory of substantive criminality as to each overt act alleged in Count 1.

Nevertheless, I am left with a concern that the defendants – and I – may not understand precisely what is being charged in Count 2. As noted above, the government has combined multiple acts in Count 2. A unanimity instruction is fine as far as it goes, but the parties and the jury must still be clear as to the range of charged acts from which the jury will be choosing. Neither the defendants nor a jury should be asked to extract what has been *charged* (as opposed to what has been *proven*) from a welter of data. I will therefore grant, in part, defendants’ request for a bill of particulars.

Within 10 days of the entry of this order, the United States shall prepare a bill of particulars

(a) listing each act of unauthorized access that is charged substantively in Count 2 and, as to each,

(b) stating whether the government contends that defendant(s) did it in furtherance of a CFAA “damage” offense;

(c) stating whether the government contends that defendant(s) did it in furtherance of state-law “harassment” offense.

No particular format is required, but the government may wish to consider a four-column chart in the following format:

Access (date/time)	Charged in Count 2? (Y/N)	In furtherance of Damage? (Y/N)	In furtherance of Harassment? (Y/N)
xx/xx/20xx 12:01 am	Y	Y	N
Etc.			

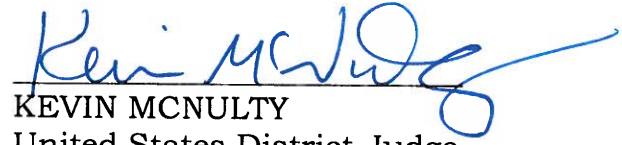
I do not mean to imply that any act not listed will be excluded from evidence; on the contrary, it may well be admissible as an integral part of the offense conduct, as an overt act in furtherance of the conspiracy, or on some other basis. Such a bill of particulars will, however, help all parties to understand the charges, as well as to design jury instructions and (if appropriate) to propose a verdict form that will ensure jury unanimity.

7. *Motion to strike a/k/a names from caption*

Defendant Joseph Roque has moved to strike from the caption the a/k/a names attributed to him: “Maria Pasquale” and “Jeffery Reynoso.” The caption, as opposed to the allegations in the body of the Indictment, is likely to be accepted by the jury as a neutral, true statement of the parties’ identities. I would be inclined to strike a/k/a names if they were, for example, associated with criminal activity or propensity. Similarly I would strike an alias that tended, at least psychologically, to vitiate the government’s burden of proof as to a contested issue (for example, that two persons were one and the same). At

oral argument, I asked defense counsel whether there would be a substantial dispute over whether his client had used the a/k/a names online; he replied that there would not. Based on that representation, I will deny the motion to strike. Should the situation change, I would entertain an application to strike the a/k/a names from any copy of the Indictment furnished to the jury.

Dated: June 6, 2013


KEVIN MCNULTY
United States District Judge